QUADRATIC RESIDUE CODES OVER $\mathbb{F}_p + v\mathbb{F}_p$ AND THEIR GRAY IMAGES

ABIDIN KAYA, BAHATTIN YILDIZ, AND IRFAN SIAP

ABSTRACT. In this paper quadratic residue codes over the ring $\mathbb{F}_p + v\mathbb{F}_p$ are introduced in terms of their idempotent generators. The structure of these codes is studied and it is observed that these codes share similar properties with quadratic residue codes over finite fields. For the case $p = 2$, Euclidean and Hermitian self-dual families of codes as extended quadratic residue codes are considered and two optimal Hermitian self-dual codes are obtained as examples. Moreover, a substantial number of good p-ary codes are obtained as images of quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$ in the cases where p is an odd prime. These results are presented in tables.

1. INTRODUCTION

Quadratic residue codes fall into the family of BCH codes and have proven to be a promising family of cyclic codes. They were first introduced by Andrew Gleason and since then have generated a lot of interest. Two famous members of this family which are Hamming and Golay codes are optimal and perfect codes. Further, as extended quadratic residue cyclic codes, extended Hamming and Golay codes also have been and are being applied in many applications in data transmission such as Voyager (1979-1981), and more recently [2, 8, 11, 17]. While initially quadratic residue codes were studied within the confines of finite fields, there have been recent developments in the form of quadratic residue codes over some special rings.

First, Pless and Qian studied quaternary quadratic residue codes (over the ring $\mathbb{Z}_4$) and some of their properties in [15]. In 2000, Chiu et al. extended the ideas in [15] to the ring $\mathbb{Z}_8$ in [7]. Recently, Taeri considered quadratic residue codes over the ring $\mathbb{Z}_9$ in [16].

Our aim in this paper is to introduce and study quadratic residue codes over the ring $\mathbb{F}_p + v\mathbb{F}_p$ which is isomorphic to $\mathbb{F}_p \times \mathbb{F}_p$. Codes over $\mathbb{F}_p + v\mathbb{F}_p$ were first introduced by Bachoc in [1] together with a new weight. They are shown to be connected to lattices and have since generated interest among coding theorists. For some of the work in the literature about these codes we refer the readers to [1, 3, 6, 9] and [4]. Recently, Zhu et al. considered the structure of cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ in [18].

We first give some preliminaries about the ring $\mathbb{F}_p + v\mathbb{F}_p$ and codes over $\mathbb{F}_p + v\mathbb{F}_p$ in Section 2. In Section 3, quadratic residue codes over the ring $\mathbb{F}_p + v\mathbb{F}_p$ are defined and it is shown that they share similar properties with quadratic residue codes over fields. In Section 4, we study the case $p = 2$ and obtain Euclidean self-dual codes

for $q = 8r - 1$ and Hermitian self-dual codes for $q = 8r + 1$ as the extended quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Two well-known optimal Hermitian self-dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$ are obtained from quadratic residue codes.

Section 5 includes the examples of QR codes for odd prime p. A number of examples including best known, optimal self-dual and extremal p-ary codes are obtained as Gray images of QR codes and the results are presented in tables.

2. Preliminaries

The ring $\mathbb{F}_p + v\mathbb{F}_p$ is a commutative ring of order p^2 and characteristic p, subject to the restriction $v^2 = v$. It is easily observed that the ring $\mathbb{F}_p + v\mathbb{F}_p$ is isomorphic to the ring $\mathbb{F}_p \times \mathbb{F}_p$. It has two maximal ideals $\langle v \rangle$ and $\langle 1 - v \rangle$. So, it is not a local ring. The ring is Frobenius, and hence is suitable for studying codes. A code C of length n over $\mathbb{F}_p + v\mathbb{F}_p$ is an $(\mathbb{F}_p + v\mathbb{F}_p)$-submodule of $(\mathbb{F}_p + v\mathbb{F}_p)^n$. An element of C is called a codeword of C. A generator matrix of C is a matrix whose rows generate C. The Hamming weight of a codeword is the number of non-zero components. Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of $(\mathbb{F}_p + v\mathbb{F}_p)^n$. The Euclidean inner product is given as $\langle x, y \rangle_E = \sum x_i y_i$. The dual code $C^\perp$ of C with respect to the Euclidean inner product is defined as

$$C^\perp = \{x \in (\mathbb{F}_p + v\mathbb{F}_p)^n \mid \langle x, y \rangle_E = 0 \text{ for all } y \in C\}$$

C is self-dual if $C = C^\perp$.

In the sequel we let $R_{p,n} := (\mathbb{F}_p + v\mathbb{F}_p)[x] / (x^n - 1)$. Where there is no confusion a polynomial $f(x)$ is abbreviated as f. An idempotent is an element $a(x)$ such that $a(x)^2 = a(x)$. We characterize all idempotents in $R_{p,n}$ in the following lemma:

Lemma 2.1. $\{(1 - v) f + vh \mid f \text{ and } h \text{ are idempotents in } \mathbb{F}_p[x]/(x^n - 1)\}$ is the set of all idempotents in $R_{p,n}$.

Proof. Let $g = (1 - v) f + vh$ be an arbitrary idempotent in $R_{p,n}$ then,

$$g = g^2 = (1 - v)^2 f^2 + v^2 h^2 \text{ (since } v(1 - v) = 0) \text{ and so we get,}$$
$$(1 - v) f + vh = (1 - v) f^2 + vh^2,$$

which implies that f and h are idempotents in $\mathbb{F}_p[x]/(x^n - 1)$.

Conversely, if f and h are idempotents in $\mathbb{F}_p[x]/(x^n - 1)$ then $(1 - v) f + vh$ is an idempotent in $R_{p,n}$, since

$$[(1 - v) f + vh]^2 = (1 - v)^2 f^2 + v^2 h^2$$
$$= (1 - v) f + vh.$$

Hence, $\{(1 - v) f + vh \mid f \text{ and } h \text{ are idempotents in } \mathbb{F}_p[x] / (x^n - 1)\}$ is the set of all idempotents in $R_{p,n}$. $\square$

In the following theorems R is a finite commutative ring with identity:

Theorem 2.2. [13][16] *Let f, g be idempotents of $R[x] / (x^n - 1)$ and let $C_1 = \langle f \rangle$, $C_2 = \langle g \rangle$ be cyclic codes over R. Then $C_1 \cap C_2$ and $C_1 + C_2$ have idempotent generators fg and $f + g - fg$, respectively.*

Theorem 2.3. [13][16] *Let $f(x)$ be the idempotent generator of an R-cyclic code C. Then $1 - f(x^{-1})$ is the idempotent generator of the dual code $C^\perp$.*

The extended code of a code C over $\mathbb{F}_p + v\mathbb{F}_p$ will be denoted by $\overline{C}$, which is the code obtained by adding a specific column to the generator matrix of C.

For the rest of this work, q is an odd prime such that p is a quadratic residue modulo q, we set $e_1(x) = \sum_{i \in Q_q} x^i$ and $e_2(x) = \sum_{i \in N_q} x^i$, where Q_q denotes the set of quadratic residues modulo q and N_q denotes the set of quadratic non-residues modulo q.

Let a be a non-zero element of $\mathbb{F}_q$, the map $\mu_a : \mathbb{F}_q \to \mathbb{F}_q$ is defined as $\mu_a(i) = ai$ (mod q). This map acts on polynomials as

$$\mu_a\left(\sum_i x^i\right) = \sum_i x^{\mu_a(i)}.$$

It is easy to see that $\mu_a(fg) = \mu_a(f)\mu_a(g)$ for polynomials f and g in $R_{p,q}$.

2.1. **Case I.** If p is an odd prime,

$$\begin{aligned} \varphi &: & \mathbb{F}_p + v\mathbb{F}_p &\to \mathbb{F}_p^2 \\ a + bv &\mapsto & (-b, 2a + b)\,. \end{aligned}$$

was defined as the Gray map in [19]. The Lee weight of an element in $\mathbb{F}_p + v\mathbb{F}_p$ is defined as the Hamming weight of its Gray image; in other words

$$w_L(a + bv) = \begin{cases} 0, \text{if } a = 0, b = 0 \\ 1, \text{if } a \neq 0, b = 0 \\ 1, \text{if } b \neq 0, 2a + b \equiv 0 \pmod{p} \\ 2, \text{if } b \neq 0, 2a + b \neq 0 \pmod{p} \end{cases}$$

The Gray map φ is extended to $(\mathbb{F}_p + v\mathbb{F}_p)^n$ componentwise, naturally.

Proposition 2.4. [19] *The Gray map φ is a distance-preserving map from $((\mathbb{F}_p + v\mathbb{F}_p)^n$, Lee distance) to $(\mathbb{F}_p^{2n}$, Hamming distance) and it is also $\mathbb{F}_p$-linear.*

Proposition 2.5. *The Gray image of a self-dual code over $\mathbb{F}_p + v\mathbb{F}_p$ is a p-ary self-dual code.*

Proof. It is enough to show that the extended Gray map preserves orthogonality, then the result follows from the size of the image. Let $\overline{a} + \overline{b}v$ and $\overline{c} + \overline{d}v$ where $\overline{a}, \overline{b}, \overline{c}$ and $\overline{d} \in \mathbb{F}_p^n$ be two codewords of length n over $\mathbb{F}_p + v\mathbb{F}_p$ such that they are orthogonal, then

$$\begin{aligned} (\overline{a} + \overline{b}v)(\overline{c} + \overline{d}v) &= 0 \\ \overline{ac} + (\overline{ad + bc + bd})v &= 0 \end{aligned}$$

Now, consider the inner product of the Gray images;

$$\begin{aligned} (-b, 2a + b)(-d, 2c + d) &= \overline{bd + 4ac + 2ad + 2bc + bd} \\ &= \overline{4ac + 2(ad + bc + bd)}. \end{aligned}$$

It is easily observed that if two codewords are orthogonal then so are their Gray images. $\square$

In [19] it was shown that $S_n := (\mathbb{F}_p + v\mathbb{F}_p)[x]/(x^n - (1 - 2v))$ is a principal ideal ring. In the following proposition we describe the cyclic codes of odd lengths in terms of ideals in S_n:

Proposition 2.6. *Let* $\psi : (\mathbb{F}_p + v\mathbb{F}_p)[x]/(x^n - 1) \to (\mathbb{F}_p + v\mathbb{F}_p)[x]/(x^n - (1 - 2v))$ *be defined as*

$$\psi(c(x)) = c((1 - 2v)x).$$

If n is odd, then ψ is a ring isomorphism from $R_{p,n}$ to S_n.

Proof. Note that $1 - 2v$ is a unit in $\mathbb{F}_p + v\mathbb{F}_p$ with $(1 - 2v)^2 = 1$. But this implies that if n is odd, then

$$(1 - 2v)^n = (1 - 2v).$$

Now, suppose $a(x) \equiv b(x) \pmod{x^n - 1}$, i.e. $a(x) - b(x) = (x^n - 1)q(x)$ for some $q(x) \in (\mathbb{F}_p + v\mathbb{F}_p)[x]$. Then

$$
\begin{aligned}
a((1 - 2v)x) - b((1 - 2v)x) &= ((1 - 2v)^n x^n - 1)q((1 - 2v)x) \\
&= \left((1 - 2v)x^n - (1 - 2v)^2\right)q((1 - 2v)x) \\
&= (1 - 2v)(x^n - (1 - 2v))q((1 - 2v)x),
\end{aligned}
$$

which means if $a(x) \equiv b(x) \pmod{x^n - 1}$, then $a((1 - 2v)x) \equiv b((1 - 2v)x)$ $\pmod{x^n - (1 - 2v)}$. The converse can easily be shown as well which means

$$a(x) \equiv b(x) \pmod{x^n - 1} \Leftrightarrow a((1 - 2v)x) \equiv b((1 - 2v)x) \pmod{x^n - (1 - 2v)}.$$

Note that one side of the implication tells us that ψ is well-defined and the other side tells us that it is injective, but since the rings are finite this proves that ψ is an isomorphism. $\square$

The following corollaries follow naturally from the proposition:

Corollary 2.7. *I is an ideal of $R_{p,n}$ if and only if $\psi(I)$ is an ideal of S_n when n is odd.*

Corollary 2.8. *Cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ of odd length are principally generated.*

2.2. **Case II.** If $p = 2$ then the Lee weight for $\mathbb{F}_2 + v\mathbb{F}_2$ is defined as

$$w_L(0) = 0, w_L(1) = 2, w_L(1 + v) = 1, w_L(v) = 1,$$

and the following Gray map is a linear isometry with respect to the Lee weight:

$$
\begin{aligned}
\varphi \quad &: \quad \mathbb{F}_2 + v\mathbb{F}_2 \to \mathbb{F}_2^2 \\
a + bv \quad &\mapsto \quad (a, a + b).
\end{aligned}
$$

The Gray map is extended componentwise and preserves self-duality [9].

In [1], Bachoc defined the following weight on $\mathbb{F}_2 + v\mathbb{F}_2$:

$$w_B(0) = 0, w_B(1) = 1, w_B(1 + v) = 2, w_B(v) = 2.$$

The weight of a codeword is the sum of the weights of its components. The minimum Hamming, Lee and Bachoc weights, d_H, d_L and d_B of C are the smallest Hamming, Lee and Bachoc weights among the non-zero codewords of C, respectively.

Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be two elements of $(\mathbb{F}_2 + v\mathbb{F}_2)^n$. The Hermitian inner product is defined as $\langle x, y \rangle_H = \sum x_i \overline{y_i}$ where $\overline{0} = 0$, $\overline{1} = 1$, $\overline{v} = 1 + v$ and $\overline{1 + v} = v$. The dual code C^* with respect to the Hermitian inner product of C is defined as

$$C^* = \{x \in (\mathbb{F}_2 + v\mathbb{F}_2)^n \mid \langle x, y \rangle_H = 0 \text{ for all } y \in C\}.$$

C is Hermitian self-dual if $C = C^*$.

The following theorems, taken from [18] characterize the structure of cyclic codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$:

Theorem 2.9. [18] *For any cyclic code C of length n over $\mathbb{F}_2 + v\mathbb{F}_2$, there is a unique polynomial $g(x)$ such that $C = \langle g(x) \rangle$, and $g(x) \mid x^n - 1$.*

Corollary 2.10. [18] *Every ideal of $R_{2,n} = (\mathbb{F}_2 + v\mathbb{F}_2)[x]/(x^n - 1)$ is principal.*

Theorem 2.11. [18] *If n is odd then every cyclic code over $\mathbb{F}_2 + v\mathbb{F}_2$ has a unique idempotent generator.*

Corollary 2.12. *Any cylic code C of odd length q over $\mathbb{F}_2 + v\mathbb{F}_2$ has a unique idempotent generator of the form $(1 + v) f + vh$ where f and h are idempotents in $\mathbb{F}_2 [x] / (x^q - 1)$.*

Proof. Since q is odd this is an immediate consequence of Theorem 2.11 and Lemma 2.1. $\square$

3. Quadratic Residue Codes over $\mathbb{F}_p + v\mathbb{F}_p$

Let q be a prime such that p is a quadratic residue in $\mathbb{F}_q$. So, QR-codes of length q over $\mathbb{F}_p$ exist. For the idempotent generators of these codes we refer to [14]. Let a and b be the idempotent generators of $\left[q, \frac{q+1}{2}\right]$ QR-codes over $\mathbb{F}_p$ and a', b' be the idempotent generators of $\left[q, \frac{q-1}{2}\right]$ QR-codes over $\mathbb{F}_p$.

Definition 3.1. Let q be a prime such that p is a quadratic residue modulo q. Set $Q_1 = \langle (1 - v) a + vb \rangle$, $Q_2 = \langle (1 - v) b + va \rangle$ and $\langle Q_1' = (1 - v) a' + vb' \rangle$, $Q_2' = \langle (1 - v) b' + va' \rangle$. These four codes are called quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$ of length q.

As in the case of QR-codes over finite fields, the properties of QR-codes over $\mathbb{F}_p + v\mathbb{F}_p$ differ for the cases $q \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$.

3.1. **Case I.** If $q \equiv 3 \pmod 4$ then the codes have the following properties.

Theorem 3.2. *With the notation as in the Definition 3.1, the following hold for $(\mathbb{F}_p + v\mathbb{F}_p)$-QR codes:*
a) *Q_1 and Q_1' are equivalent to Q_2 and Q_2', respectively;*
b) *$Q_1 \cap Q_2 = \langle h \rangle$ and $Q_1 + Q_2 = R_{p,q}$ where $h = 1 + e_1 + e_2$ is the polynomial corresponding to the all one vector of length q;*
c) *$|Q_1| = p^{(q+1)} = |Q_2|$;*
d) *$Q_1 = Q_1' + \langle h \rangle , \; Q_2 = Q_2' + \langle h \rangle$;*
e) *$|Q_1'| = p^{(q-1)} = |Q_2'|$;*
f) *Q_1' and Q_2' are self-orthogonal and $Q_1^{\perp} = Q_1'$ and $Q_2^{\perp} = Q_2'$;*
g) *$Q_1' \cap Q_2' = \{0\}$ and $Q_1' + Q_2' = \langle 1 + h \rangle$.*

Proof.
a) Let $n \in N_q$ then $\mu_n a = b$ and $\mu_n a' = b'$ therefore

$$\mu_n [(1 - v) a + vb] = (1 - v) b + va$$

so Q_1 and Q_2 are equivalent. Similarly,

$$\mu_n [(1 - v) a' + vb'] = (1 - v) b' + va'$$

which implies Q_1' and Q_2' are equivalent.

b) $Q_1 \cap Q_2$ has idempotent generator

$$[(1-v)\,a + vb]\,[(1-v)\,b + va] = (1-v)\,ab + vab = ab = h$$

and $Q_1 + Q_2$ has idempotent generator $(1-v)\,a + vb + (1-v)\,b + va - ab = a + b - ab = 1$.

c) By a) and b) we have

$$\left(p^2\right)^q = |Q_1 + Q_2| = \frac{|Q_1|\,|Q_2|}{|Q_1 \cap Q_2|} = \frac{|Q_1|^2}{p^2},$$

so $|Q_1| = |Q_2| = p^{(q+1)}$.

d) $Q_1' + \langle h \rangle$ has idempotent generator

$$(1-v)\,a' + vb' + h - [(1-v)\,a' + vb']\,h$$
$$= (1-v)\,[a' + h - a'h] + v\,[b' + h - b'h] = (1-v)\,a + vb$$

Hence, $Q_1' + \langle h \rangle = Q_1$. Similarly, $Q_2 = Q_2' + \langle h \rangle$.

e) $p^{(q+1)} = |Q_1| = |Q_1' + \langle h \rangle| = |Q_1'|\,|\langle h \rangle| = p^2\,|Q_1'|$. Thus $|Q_1'| = p^{(q-1)}$.

f) $Q_1^\perp$ has idempotent generator $1 - \left((1-v)\,a\left(x^{-1}\right) + vb\left(x^{-1}\right)\right)$ and since $-1 \in N_q$, $a\left(x^{-1}\right) = b$ and $b\left(x^{-1}\right) = a$. So we obtain

$$1 - \left((1-v)\,a\left(x^{-1}\right) + vb\left(x^{-1}\right)\right) = 1 - v + (1-v)\,a\left(x^{-1}\right) + v - vb\left(x^{-1}\right)$$
$$= (1-v)\left[1 - a\left(x^{-1}\right)\right] + v\left[1 - b\left(x^{-1}\right)\right]$$
$$= (1-v)\,a' + vb'.$$

which implies $Q_1^\perp = Q_1'$. Similarly, $Q_2^\perp = Q_2'$. By d) $Q_1' \subset Q_1$ and $Q_2' \subset Q_2$ it follows that they are self orthogonal.

g) $Q_1' \cap Q_2'$ has idempotent generator

$$[(1-v)\,a' + vb']\,[(1-v)\,b' + va']$$
$$= (1-v)\,a'b' + va'b'$$
$$= a'b' = 0.$$

$Q_1' + Q_2'$ has idempotent generator $(1-v)\,a' + vb' + (1-v)\,b' + va' - 0 = a' + b' = 1 + h$. $\qquad\square$

In the following, the extended QR-codes over $\mathbb{F}_p + v\mathbb{F}_p$ are formed by adding the same columns that are used to extend QR-codes over $\mathbb{F}_p$.

Theorem 3.3. *Suppose $q \equiv 3 \pmod 4$ and Q_1, Q_2 are $\mathbb{F}_p + v\mathbb{F}_p$-QR codes as given in Definition 3.1. Then $\overline{Q_1}$ and $\overline{Q_2}$ are self-dual.*

Proof. If $p \equiv 1 \pmod 4$ then both -1 and q are quadratic residues in $\mathbb{F}_p$. If $p \equiv 3 \pmod 4$ then both -1 and q are non-residues in $\mathbb{F}_p$. These follow easily from the quadratic reciprocity law. So, in any case $-q$ is a quadratic residue in $\mathbb{F}_p$, i.e. there exists $r \in \mathbb{F}_p$ such that $r^2 = -q$. By Theorem 3.2, $Q_1 = Q_1' + \langle h \rangle$. Let $\overline{Q_1}$ be the code generated by

$$
\begin{array}{ccccccc}
\infty & 0 & 1 & 2 & \cdots & q-1 &
\end{array}
$$

(3.1)
$$
\begin{pmatrix}
0 & & & & & & \\
0 & & & G_1' & & & \\
\vdots & & & & & & \\
r & 1 & 1 & 1 & \cdots & 1 &
\end{pmatrix}
$$

where G'_1 is a generator matrix for Q'_1 and r is an element with $r^2 \equiv -q \pmod{p}$. Note that the all 1 vector is in Q_1. Hence, since $Q_1^\perp = Q'_1$, the last row is orthogonal to the rows above; moreover it is orthogonal to itself, making the code $\overline{Q_1}$ self-orthogonal. By comparing $\left|\overline{Q_1}\right|$ and $\left|\overline{Q_1}^\perp\right|$ it follows that $\overline{Q_1}$ is self-dual. Similarly, $\overline{Q_2}$ is self-dual. □

3.2. **Case II.** If $q \equiv 1 \pmod 4$ then the codes have the following properties.

Theorem 3.4. *With the notation as in the Definition 3.1, the following hold for* $(\mathbb{F}_p + v\mathbb{F}_p)$*-QR codes:*
a) *Q_1 and Q'_1 are equivalent to Q_2 and Q'_2, respectively;*
b) *$Q_1 \cap Q_2 = \langle h \rangle$ and $Q_1 + Q_2 = R_{p,q}$ where $h = 1 + e_1 + e_2$;*
c) *$|Q_1| = p^{(q+1)} = |Q_2|$;*
d) *$Q_1 = Q'_1 + \langle h \rangle$, $Q_2 = Q'_2 + \langle h \rangle$;*
e) *$|Q'_1| = p^{(q-1)} = |Q'_2|$;*
f) *$Q_1^\perp = Q'_2$ and $Q_2^\perp = Q'_1$;*
g) *$Q'_1 \cap Q'_2 = \{0\}$ and $Q'_1 + Q'_2 = \langle 1 + h \rangle$.*

Proof. The proof is similar to the proof of Theorem 3.2 and hence is omitted here. □

We finish this section with the following theorem describing the duality relation between the extended quadratic residue codes:

Theorem 3.5. *Suppose $q \equiv 1 \pmod 4$ and Q_1, Q_2 are $\mathbb{F}_p + v\mathbb{F}_p$-QR codes as given in Definiton 3.1. Then the dual of $\overline{Q_1}$ is $\overline{Q_2}$ and the dual of $\overline{Q_2}$ is $\overline{Q_1}$.*

Proof. Since, $Q_i = Q'_i + \langle h \rangle$ for $i = 1, 2$, $\overline{Q_i}$ can be defined as the code generated by the following matrix $\overline{G_i}$;

$$
\begin{array}{cccccc}
\infty & 0 & 1 & 2 & \cdots & q-1
\end{array}
$$

$$
\begin{pmatrix}
0 & & & & & \\
0 & & & G'_i & & \\
\vdots & & & & & \\
g_i & 1 & 1 & 1 & \cdots & 1
\end{pmatrix}
$$

where G'_i is a generator matrix of Q'_i and $g_1 = 1, g_2 = -q$. By Theorem 3.4 $Q_2^\perp = Q'_1$ and $Q_1^\perp = Q'_2$. Since the all 1 vector is in both Q_1 and Q_2, this implies that it is orthogonal to both G'_1 and G'_2. Moreover, the last row of $\overline{G_1}$ is orthogonal to the last row of $\overline{G_2}$. It follows that the codes are orthogonal to each other. By comparing their orders we see that $\overline{Q_1}^\perp = \overline{Q_2}$. □

Recall that Q_1 and Q_2 are equivalent and thus have the same weight enumerator. Since $w_L(1) = w_L(-q)$, $\overline{Q_1}$ and $\overline{Q_2}$ have the same weight enumerator. Thus, by theorems 3.3 and 3.5 and proposition 2.5 we obtain the following corollary:

Corollary 3.6. *The Gray images of the extended quadratic residue codes over* $\mathbb{F}_p + v\mathbb{F}_p$ *are self-dual codes if $q \equiv 3 \pmod 4$ and formally self-dual codes if $q \equiv 1$* *(mod 4).*

4. Quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$, extended quadratic residue codes and binary images

In this section, we define extended quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$. Further, we provide two optimal Hermitian self-dual codes as applications to the main theorems.

Proposition 4.1. [4] *Let d_H and d_L be the minimum Hamming and Lee weights of $C = (1 + v) C_1 \oplus vC_2$, respectively. Then*

$$d_H(C) = d_L(C) = \min\{d(C_1), d(C_2)\}$$

where $d(C_i)$ denotes the minimum weight of the binary code C_i.

A self-dual code is called Type IV if all the Hamming weights are even, a binary code is called even if all the weights are even.

Proposition 4.2. [1] [9] *If $C = (1 + v) C_1 \oplus vC_2$ then C is Euclidean self-dual if and only if C_1 and C_2 are binary self-dual codes. $C = (1 + v) C_1 \oplus vC_2$ is Euclidean Type IV self-dual if and only if $C_1 = C_2$.*

Proposition 4.3. [1] [9] *If $C = (1 + v) C_1 \oplus vC_2$ then C is Hermitian self-dual if and only if $C_1 = C_2^{\perp}$. $C = (1 + v) C_1 \oplus vC_1^{\perp}$ is Hermitian Type IV self-dual if and only if C_1 and $C_1^{\perp}$ are even codes.*

The following gives an upper bound on the Bachoc distances of Hermitian self-dual codes.

Theorem 4.4. [1] *Let C be a Hermitian self-dual code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ then $w_B(C) \leq 2([n/3] + 1)$.*

Codes that meet this bound are called extremal codes and Bachoc has shown that they correspond to extremal modular lattices.

4.1. **Case I.** If $q = 8r - 1$ then e_1 and e_2 are generating idempotents of $\left[q, \frac{q+1}{2}\right]$ binary quadratic residue codes and $e_1 e_2 = h$.

In this case, the $(\mathbb{F}_2 + v\mathbb{F}_2)$-QR codes turn out to have the following form.

Definition 4.5. If $q = 8r - 1$ let $Q_1 = \langle (1 + v) e_1 + ve_2 \rangle$, $Q_2 = \langle (1 + v) e_2 + ve_1 \rangle$ and $Q_1' = \langle (1 + v) (1 + e_2) + v (1 + e_1) \rangle$, $Q_2' = \langle (1 + v) (1 + e_1) + v (1 + e_2) \rangle$. These four codes are called quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$ of length q.

Example 4.6. For $q = 7$ the QR-code Q_1 is generated by the idempotent $e = (1 + v)\left(x + x^2 + x^4\right) + v\left(x^3 + x^5 + x^6\right)$ in $R_{2,7}$. As the extended QR-code $\overline{Q_1}$ we get the self-dual code which is generated by

$$\begin{pmatrix} 0 & 1 & 1+v & 1+v & v & 1+v & v & v \\ 0 & v & 1 & 1+v & 1+v & v & 1+v & v \\ 0 & v & v & 1 & 1+v & 1+v & v & 1+v \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

with $d_L\left(\overline{Q_1}\right) = 4$ and $d_B\left(\overline{Q_1}\right) = 7$. So its Gray image corresponds to a $[16, 8, 4]$ optimal self-dual binary code. $\overline{Q_1}$ has Lee weight enumerator

$$1 + 28z^4 + 198z^8 + 28z^{12} + z^{16},$$

Hamming weight enumerator

$$1 + 28z^4 + 56z^5 + 84z^6 + 56z^7 + 31z^8,$$

and Bachoc weight enumerator

$$1 + 56z^7 + 29z^8 + 84z^{10} + 28z^{12} + 56z^{13} + 2z^{16}.$$

Example 4.7. For $q = 23$, the extended quadratic residue code $\overline{Q_1}$ is a self-dual code with $d_B\left(\overline{Q_1}\right) = 14$, $d_H\left(\overline{Q_1}\right) = 8 = d_L\left(\overline{Q_1}\right)$ and Lee weight enumerator

$$1 + 1518z^8 + 5152z^{12} + 577599z^{16} + 3910368z^{20} + 7787940z^{24}$$

$$+3910368z^{28} + 577599z^{32} + 5152z^{36} + 1518z^{40} + z^{48}.$$

4.2. **Case II.** If $q = 8r + 1$ then e_1 and e_2 are generating idempotents of $\left[q, \frac{q-1}{2}\right]$ binary quadratic residue codes and $e_1 e_2 = 0$.

In this case, the $(\mathbb{F}_2 + v\mathbb{F}_2)$-QR codes turn out to have the following form.

Definition 4.8. If $q = 8r + 1$ let $Q_1 = \langle (1+v)(1+e_1) + v(1+e_2) \rangle$, $Q_2 = \langle (1+v)(1+e_2) + v(1+e_1) \rangle$ and $Q'_1 = \langle (1+v)e_2 + ve_1 \rangle$, $Q'_2 = \langle (1+v)e_1 + ve_2 \rangle$. These four codes are called quadratic residue codes over $\mathbb{F}_2 + v\mathbb{F}_2$ of length q.

In the next theorem we introduce a family of Hermitian self-dual codes by using quadratic residue codes:

Theorem 4.9. *Suppose $q = 8r + 1$ and Q'_1, Q'_2 are $\mathbb{F}_2 + v\mathbb{F}_2$-QR codes as given in Definition 4.8. Then $Q'_1 + \langle \boldsymbol{v} \rangle$, $Q'_2 + \langle \boldsymbol{v} \rangle$, $Q'_1 + \langle \boldsymbol{1 + v} \rangle$ and $Q'_2 + \langle \boldsymbol{1 + v} \rangle$ are Hermitian self-dual codes of length q where $\boldsymbol{v}$ denotes the polynomial vh which corresponds to the all-v vector of length q and $\boldsymbol{1 + v}$ denotes the polynomial $(1 + v)h$ which corresponds to the all-$(1 + v)$ vector.*

Proof. $Q'_1 + \langle \boldsymbol{v} \rangle$ has idempotent generator

$$(1+v)e_2 + ve_1 + \boldsymbol{v} - ((1+v)e_2 + ve_1)\boldsymbol{v}$$
$$= e_2 + ve_2 + ve_1 + v + ve_1 + ve_2 - ve_1 v(1 + e_1 + e_2)$$
$$= e_2 + v - v^2 e_1 - v^2 e_1^2 - v^2 e_1 e_2$$
$$= e_2 + v - ve_1 - ve_1 - 0$$
$$= e_2 + v$$
$$= (1+v)e_2 + v(1+e_2)$$

So, $Q'_1 + \langle \boldsymbol{v} \rangle = (1+v)C_1 \oplus vC_2$ where $C_1 = \langle e_2 \rangle$ and $C_2 = \langle 1 + e_2 \rangle$. $C_2^{\perp}$ has idempotent generator $1 - \left(1 + e_2\left(x^{-1}\right)\right) = e_2\left(x^{-1}\right) = e_2$ since $-1 \in Q_q$, it follows that $C_1 = C_2^{\perp}$. Hence, by Proposition 4.3. $Q'_1 + \langle \boldsymbol{v} \rangle$ is Hermitian self-dual. Similarly, $Q'_2 + \langle \boldsymbol{v} \rangle$ is Hermitian self-dual.

$Q'_1 + \langle \boldsymbol{1 + v} \rangle$ has idempotent generator

$$(1+v)e_2 + ve_1 + \boldsymbol{1 + v} - ((1+v)e_2 + ve_1)(\boldsymbol{1 + v})$$
$$= 1 + v + e_1 - (1+v)e_2(1 + e_1 + e_2)$$
$$= 1 + v + e_1 - (1+v)(e_2 + 0 + e_2)$$
$$= 1 + v + e_1$$
$$= (1+v)(1+e_1) + ve_1.$$

So, $Q'_1 + \langle \boldsymbol{1 + v} \rangle = (1+v)C_1 \oplus vC_2$ where $C_1 = \langle 1 + e_1 \rangle$ and $C_2 = \langle e_1 \rangle$. $C_2^{\perp}$ has idempotent generator $1 - e_1\left(x^{-1}\right) = 1 - e_1 = 1 + e_1$. Hence, by Proposition 4.3 $Q'_1 + \langle \boldsymbol{1 + v} \rangle$ is Hermitian self-dual. Similarly, $Q'_2 + \langle \boldsymbol{1 + v} \rangle$ is Hermitian self-dual. $\square$

Example 4.10. For $q = 17$, the code $Q'_1 + \langle v \rangle$ is the unique optimal Hermitian self-dual code of length 17 with $d_B (Q'_1 + \langle v \rangle) = 10$ and Bachoc weight enumerator

$$1 + 187z^{10} + 1156z^{12} + 2924z^{14} + 10030z^{16} + 18513z^{18} + 27744z^{20}$$
$$+ 29954z^{22} + 23188z^{24} + 12019z^{26} + 850z^{30} + 85z^{32} + z^{34}.$$

Theorem 4.11. *Suppose $q = 8r + 1$ and Q_1, Q_2 are $\mathbb{F}_2 + v\mathbb{F}_2$-QR codes as given in Definition 4.8. Then $\overline{Q_1}$ and $\overline{Q_2}$ are Hermitian self-dual codes.*

Proof. By Theorem 3.4 $Q_1 = Q'_1 + \langle h \rangle$, and $\overline{Q_1}$ has the $\frac{q+1}{2} \times (q+1)$ generator matrix (3.1). By Theorem 4.9. $Q'_1 + \langle v \rangle$ is Hermitian self-dual and it is easily seen that any row of this generator matrix is orthogonal to all-1 vector since $|Q_q| = |N_q| = \frac{q-1}{2} = 4r$ and all-1 vector is orthogonal to itself with respect to Hermitian inner product. Therefore $\overline{Q_1}$ is Hermitian self-dual. Similarly, $\overline{Q_2}$ is Hermitian. $\square$

Example 4.12. For $q = 17$, the extended quadratic residue code $\overline{Q_1}$ is the unique optimal Hermitian self-dual code of length 18 with $d_B (\overline{Q_1}) = 12$ and Bachoc weight enumerator

$$1 + 1734z^{12} + 1836z^{14} + 13158z^{16} + 23869z^{18} + 46818z^{20} + 55080z^{22}$$
$$+ 57324z^{24} + 37026z^{26} + 18054z^{28} + 6324z^{30} + 756z^{32} + 153z^{34} + 2z^{36}$$

$d_H (\overline{Q_1}) = 6 = d_L (\overline{Q_1})$ and $\overline{Q_1}$ is an optimal Hermitian Type IV self-dual code of length 18 as given in [4].

In [3] it is proven that there are no extremal codes with respect to the Bachoc weight for the lengths greater than 10, a self-dual code is called optimal if it has the best possible distance. Betsumiya et. al. obtained unique optimal Hermitian self-dual codes for lengths 17 and 18 which are obtained by quadratic residue codes in a different way in the examples 4.12 and 4.10.

5. EXAMPLES OF QUADRATIC RESIDUE CODES OVER $\mathbb{F}_p + v\mathbb{F}_p$, FOR ODD PRIME p

In this section, we investigate the examples of QR-codes over $\mathbb{F}_p + v\mathbb{F}_p$ for odd prime p. We obtain some extremal and optimal self-dual codes over $\mathbb{F}_p$ as Gray images of the extended QR-codes over $\mathbb{F}_p + v\mathbb{F}_p$. By $QR_p(q)$ we denote the $[q, \frac{q+1}{2}]$-quadratic residue code of length q over $\mathbb{F}_p + v\mathbb{F}_p$. As usual the notation $\overline{QR_p(q)}$ is used for the extended QR-code.

Example 5.1. For $p = 3$ and $q = 11$ we get the $(\mathbb{F}_3 + v\mathbb{F}_3)$-QR code $QR_3(11)$ which is generated by the matrix

$$\begin{pmatrix} 0 & a & v & a & a & a & v & v & v & a & v \\ v & 0 & a & v & a & a & a & v & v & v & a \\ a & v & 0 & a & v & a & a & a & v & v & v \\ v & a & v & 0 & a & v & a & a & a & v & v \\ v & v & a & v & 0 & a & v & a & a & a & v \\ v & v & v & a & v & 0 & a & v & a & a & a \end{pmatrix}$$

where $a = 1 + 2v$. It has minimum Lee distance 7, so it corresponds to a $[22, 12, 7]_3$ optimal code. Moreover, $\overline{QR_3(11)}$ has minimum Lee distance 9 and it is self-dual so its Gray image is an extremal code with parameters $[24, 12, 9]_3$. Note that this coincides with the extended QR-code over $\mathbb{F}_3$.

Example 5.2. For $p = 3$ and $q = 23$, the Gray image of $QR_3(23)$ corresponds to an optimal $[46, 24, 13]_3$ code and the image of $\overline{QR_3(23)}$ corresponds to an extremal self-dual $[48, 24, 15]_3$-code which coincides with the extended QR-code over $\mathbb{F}_3$.

Example 5.3. For $p = 5$ and $q = 11$, $QR_5(11)$ is generated by the idempotent $(1 + 4v)(1 + 2e_1 + 4e_2) + v(1 + 2e_2 + 4e_1)$ and its Gray image is a $[22, 12, 7]_5$-code which is optimal. The image of $\overline{QR_5(11)}$ is the unique optimal self-dual $[24, 12, 9]_5$ code with weight enumerator;

$$1 + 1056z^9 + 11018z^{10} + 36960z^{11} + 212352z^{12} + \cdots .$$

Example 5.4. For $p = 5$ and $q = 19$, $QR_5(19)$ is generated by the idempotent $(1 + 4v)4e_1 + v4e_2$ and its image is a $[38, 20, 11]_5$-code which is optimal. $\overline{QR_5(19)}$ is self-dual and its Gray image corresponds to an optimal self-dual code with parameters $[40, 20, 13]_5$.

Example 5.5. For $p = 7$ and $q = 19$, $QR_7(19)$ has generating idempotent $(1 + 6v)(2 + 4e_1 + 6e_2) + v(2 + 4e_2 + 6e_1)$. We obtain a self-dual code of parameters $[40, 20, 13]_7$ as the Gray image of $\overline{QR_7(19)}$.

We finish this section by combining the codes obtained in the following tables:

Table 1: QR codes for $p = 3, 5$ and 7

	The code over $\mathbb{F}_p + v\mathbb{F}_p$	Gray image; over $\mathbb{F}_p$
$QR_3(11)$	$(11, 9^6, 7)$	$[22, 12, 7]_3^*$
$\overline{QR_3(11)}$	$(12, 9^6, 9)$	$[24, 12, 9]_3^*$ extremal self-dual
$QR_3(13)$	$(13, 9^7, 7)$	$[26, 14, 7]_3^*$
$\overline{QR_3(13)}$	$(14, 9^7, 8)$	$[28, 14, 8]_3$ formally self-dual
$QR_3(23)$	$(23, 9^{12}, 13)$	$[46, 24, 13]_3^*$
$\overline{QR_3(23)}$	$(24, 9^{12}, 15)$	$[48, 24, 15]_3^*$ extremal self-dual
$QR_3(37)$	$(37, 9^{19}, 14)$	$[74, 38, 14]_3$
$\overline{QR_3(37)}$	$(38, 9^{19}, 16)$	$[76, 38, 16]_3$ formally self-dual
$QR_5(11)$	$(11, 25^6, 7)$	$[22, 12, 7]_5$
$\overline{QR_5(11)}$	$(12, 25^6, 9)$	$[24, 12, 9]_5^*$ optimal self-dual
$QR_5(19)$	$(19, 25^{10}, 11)$	$[38, 20, 11]_5^*$
$\overline{QR_5(19)}$	$(20, 25^{10}, 13)$	$[40, 20, 13]_5^*$ optimal self-dual
$QR_5(29)$	$(29, 25^{15}, 13)$	$[58, 30, 13]_5$
$\overline{QR_5(29)}$	$(30, 25^{15}, 14)$	$[60, 30, 14]_5$ formally self-dual
$QR_5(31)$	$(31, 25^{16}, 16)$	$[62, 32, 16]_5$
$\overline{QR_5(31)}$	$(32, 25^{16}, 18)$	$[64, 32, 18]_5^*$ optimal self-dual
$QR_7(3)$	$(3, 49^2, 3)$	$[6, 4, 3]_7^*$
$\overline{QR_7(3)}$	$(4, 49^2, 4)$	$[8, 4, 4]_7$ self-dual
$QR_7(19)$	$(19, 49^{10}, 11)$	$[38, 20, 11]_7$
$\overline{QR_7(19)}$	$(20, 49^{10}, 13)$	$[40, 20, 13]_7$ self-dual

In the table, $*$ denotes that the code has the best possible minimum distance by [12]. Optimal self-dual codes in the above table coincides with the quadratic double circulant (QDC) codes constructed by Gaborit in [10]. Some examples of extended QR codes for larger primes are given in the following table;

Table 2: QR codes for $p = 11, 13, 17, 19, 23$ and 29

	The code over $\mathbb{F}_p + v\mathbb{F}_p$	Gray image; over $\mathbb{F}_p$
$\overline{QR_{11}}(5)$	$(6, 121^3, 5)$	$[12, 6, 5]_{11}$ formally self-dual
$\overline{QR_{11}}(7)$	$(8, 121^4, 7)$	$[16, 8, 7]_{11}$ self-dual
$\overline{QR_{11}}(19)$	$(20, 121^{10}, 13)$	$[40, 20, 13]_{11}$ self-dual
$\overline{QR_{13}}(3)$	$(8, 169^2, 4)$	$[8, 4, 4]_{13}$ self-dual, $C_{13,8,10}$ in [5]
$\overline{QR_{13}}(17)$	$(18, 169^9, 12)$	$[36, 18, 12]_{13}$ formally self-dual
$\overline{QR_{17}}(13)$	$(14, 289^{14}, 10)$	$[28, 14, 10]_{17}$ formally self-dual
$\overline{QR_{17}}(19)$	$(20, 289^{10}, 13)$	$[40, 20, 13]_{17}$ self-dual
$\overline{QR_{19}}(3)$	$(4, 361^2, 4)$	$[8, 4, 4]_{19}$ self-dual
$\overline{QR_{19}}(5)$	$(6, 361^3, 6)$	$[12, 6, 6]_{19}$ formally self-dual
$\overline{QR_{23}}(7)$	$(8, 529^4, 7)$	$[16, 8, 7]_{23}$ self-dual
$\overline{QR_{29}}(5)$	$(6, 841^3, 6)$	$[12, 6, 6]_{29}$ formally self-dual
$\overline{QR_{29}}(7)$	$(8, 841^4, 7)$	$[16, 8, 7]_{29}$ self-dual

Self-dual codes up to length 20 in the above table are not optimal by [5].

References

[1] Bachoc, C., "Application of coding theory to the construction of modular lattices", *J. Combin. Theory Ser. A*, Vol. 78, pp. 92-119, 1997.

[2] Bae, M.H., Lee, W.Y., Jeong, M.K., Kwon, S.J. K, "Orthogonal Golay code based ultrasonic imaging without reducing frame rate", *Ultrasonics*, Vol. 2, Issue: c, pp. 1705-1708, 2002.

[3] Betsumiya, K., Gulliver, T.A., Harada, M., "Extremal self-dual codes over $\mathbb{F}_2 \times \mathbb{F}_2$", *Designs Codes and Cryptography*, Vol. 28, no.2, pp. 171-186, 2003.

[4] Betsumiya, K., Harada M., "Optimal self-dual codes over $\mathbb{F}_2 \times \mathbb{F}_2$ with respect to the Hamming weight", *IEEE Trans. Inf. Theory*, Vol.50, No.2, pp. 356–358, 2004.

[5] Betsumiya, K., Georgiou, S., Gulliver, T. A., Harada, M., Koukouvinos, C., "On self-dual codes over some prime fields", Discrete Mathematics, Vol. 262, no. 1, pp. 37-58, 2003.

[6] Bonnecaze, A., Solé, P., Calderbank, A.R., "Quaternary quadratic residue codes and unimodular lattices", *IEEE Trans. Inf. Theory*, Vol. 41, No.2, pp. 366–377, 1995.

[7] Chiu, M.H., Yau, S.T. , Yu, Y., "$\mathbb{Z}_8$-cyclic codes and quadratic residue codes", *Adv. Appl. Math*, Vol. 25, pp.12–33, 2000.

[8] O'Donovan, T.L., Acevedo Contla, P., Das-Gupta, D.K., "Application of Golay codes and piezoelectric ultrasound transducer to biomedical noninvasive measurement", *IEEE Transactions on Electrical Insulation*, Vol. 28, Issue 1, pp. 93 - 100, Feb 1993.

[9] Dougherty, S.T., Gaborit, P., Harada, M., Munemasa, A. , Sole, P., "Type IV self dual codes over rings", *IEEE Trans. Inform. Theory*, Vol. 45, No.7, pp. 2345–2360, 1999.

[10] Gaborit, P., "Quadratic double circulant codes over fields", Vol. 97, Issue 1, pp. 85-107, 2002.

[11] Garcia-Rodriguez, M., Yañez, Y., Garcia-Hernandez, M.J., Salazar, J., Turo, A., Chavez, J.A., "Application of Golay codes to improve the dynamic range in ultrasonic Lamb waves air-coupled systems", *NDT & E International*, Vol. 43, Issue 8, pp. 677–686, Nov. 2010.

[12] Grassl, M., htttp://codetables.de, accessed 04.11.2012.

[13] Huffman, W.C. and Pless, V., "Fundamentals of error correcting codes", *Cambridge University press*, 2003.

[14] MacWilliams, F.J. and Sloane, N.J.A., "The Theory of Error-Correcting Codes", North-Holland: New York, NY, 1977.

[15] Pless, V., Qian, Z., "Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$", *IEEE Trans. Inform. Theory*, Vol.42, No.5, pp. 1594-1600, 1996.

[16] Taeri, B., "Quadratic Residue Codes over $\mathbb{Z}_9$", *J. Korean Math. Soc.*, Vol.46, No.1, pp. 13-30, 2009.

[17] Trots, I., Tasinkevych, Y., Nowicki, A., Lewandowski, M., "Golay coded sequences in synthetic aperture imaging systems", *Archives of Acoustics*, Vol. 36, 4, 913–926, 2011.

[18] Zhu, S.X., Wang, Y., Shi, M.J. , "Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$", *IEEE Trans. Inf. Theory*, Vol. 56, No.4, pp. 1680–1684, 2010.

[19] Zhu, S.X., Wang, L., "A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image", *Discrete Mathematics*, Vol. 311, pp. 2677–2682, 2011.

ABIDIN KAYA, DEPARTMENT OF MATHEMATICS, FATIH UNIVERSITY, 34500, ISTANBUL, TURKEY
E-mail address: `akaya@fatih.edu.tr`

BAHATTIN YILDIZ, DEPARTMENT OF MATHEMATICS, FATIH UNIVERSITY, 34500, ISTANBUL, TURKEY
E-mail address: `byildiz@fatih.edu.tr`

IRFAN SIAP, DEPARTMENT OF MATHEMATICS, YILDIZ TECHNICAL UNIVERSITY, 34210, ISTANBUL, TURKEY
E-mail address: `isiap@yildiz.edu.tr`